

AMENDMENTS TO THE SPECIFICATION

The paragraph on page 2, lines 11-22, is amended as follows:

In one embodiment of the present invention a simplified user authentication to a computer resource is provided utilizing a smart card. When a new user is issued a smart card, he or she is also issued a user name (ID) and password to be used during a first use to activate the smart card. The user then connects the smart card and enters the user ID and password. The user is authenticated using the user ID and password and identifying information from the smart card. The network administration server then requests a public key from the workstation. The workstation instructs the smart card to ~~generates~~ generate public and private ~~key~~ keys. The public key is transmitted to the server. A digital certificate is created and the smart card is activated. Once the smart card is activated a simplified login procedure can be used wherein connecting the smart card to a workstation initiates a login process not requiring use of a PIN number or other user input.

The paragraph beginning at page 5, line 24, and continuing to page 6, line 11, is amended as follows:

Turning now to FIGURE 1, an exemplary network 100 is illustrated. A smart card 110 can be inserted into an appropriate connector in a smart card reader 114. Smart card reader 114 is connected to, or forms apart of, a workstation 120 connected to a computer network 126. Access to the network resources and issuance of smart cards, passwords, login

identification, etc. is administered using an administration server 130 which is coupled to network information services or directory services (NIS/DS) database 134. In network 100, administration server 130 also provides the function of administration of digital certificates. Smart card 110 is utilized by a user to obtain access to any of the computing resources available in network 126 including various file servers and the like. Depending upon the level of security required, it may be desirable to permit a user to login using smart card 110 as the only authentication mechanism. That is, while conventional security systems require a smart card 110 in combination with personal identification number PIN, in less secure situations it may be useful to permit connection of the smart card 110 to initiate a user login. Moreover, it may also be desirable to permit a user to activate a smart card 110 without intensive involvement of network administration ~~personal~~ personnel.

The paragraph on page 8, lines 11-27, is amended as follows:

Process 230 of FIGURE 6 describes use of a smart card 110 as an aide to simplified login and to provide authentication starting at 604. At 610, the process determines if the smart card 110 is connected, and if not, awaits connection of a smart card 110. Once a smart card 110 is connected to the workstation 120 at 610, the smart card 110, in conjunction with the workstation 120, initiates a login at 616. This may be accomplished, for example, by sending a message out over the network alerting network servers that a smart card 110 is connected. The smart card 110 is then authenticated at 620. This may be accomplished, for example, by

challenging the smart card 110 to carry out ~~and~~ an encryption operation using its private key. If the encrypted information can be correctly decrypted at the server using the public key, then it is presumed ~~to~~ that the smart card 110 is properly authenticated. The authentication process of 620 also utilizes the digital certificate and verifies that the certificate has not been revoked at 640 as a further portion of the authentication process. If the certificate is not good (for example if the certificate is indicated as having been revoked by its presence on a certificate revocation list) the login is rejected at 654. If the certificate is good at 648, login is authorized at 660 and process ends at 668.